UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,127	01/14/2000	Alan Dowd	105.176US1	7964

21186 7590 08/13/2003

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
CRAIG, DWIN M	

ART UNIT	PAPER NUMBER
2123	10

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/483,127	DOWD ET AL.	
	Examiner	Art Unit	
	Dwin M Craig	2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-42 have been presented for reconsideration in view of applicant's amended claims. Claims 1-42 have been reconsidered and rejected.

Response to Arguments

2. Applicant's arguments with respect to **Claims 1-37** have been considered but are moot in view of the new ground(s) of rejection. The Examiner asserts that the earlier rejections of **Claims 1-37** are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Independent **Claims 1 and 18** and dependent **Claims 2, 4, 5, 8 and 19** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362.**

3.1 As regards independent **Claims 1 and 18** the *Gleichauf et al.* reference discloses a security modeling system **(Col. 2 Lines 47-50, Col. 4 Lines 20-43),** a network configuration module having network configuration data **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a

computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

3.2 As regards dependent **Claim 2** the *Gleichauf et al.* reference discloses a database, including network vulnerability and exploitation data and attack data **(Figure 2 ITEM 80, Figure 3A ITEM 98, Figure 3B, 4 and 5, Col. 4 Lines 9-19, Col. 8 Lines 13-25).**

3.3 As regards dependent **Claims 4 and 19** the *Gleichauf et al.* reference discloses a network configuration discovery tool **(Figure 3A, ITEMS 90 and 92, Col. 2 Lines 6-15).**

3.4 As regards dependent **Claim 5** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

3.5 As regards dependent **Claim 8** the *Gleichauf et al.* reference discloses a portable modeling system **(Figure 1 ITEMS 20, 22, 24 and 26).**

4. Dependent **Claims 3 and 6** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

4.1 As regards independent **Claim 1** see paragraph 3.1 above.

4.2 As regards dependent **Claim 2** see paragraph 3.2 above.

4.3 As regards dependent **Claim 3** the *Gleichauf et al.* reference does not expressly disclose database tables.

The *G2* reference discloses database tables **(Figure 3B and 3C).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2*

reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

4.4 As regards dependent **Claim 6** the *Gleichauf et al.* reference does not expressly disclose receiving the network vulnerability, attack and exploitation data.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

5. Dependent **Claim 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Sparks, II U.S. Patent 6,352,479.**

5.1 As regards independent **Claim 1** see paragraph 3.1 above.

5.2 As regards dependent **Claim 7** the *Gleichauf et al.* reference does not expressly disclose a simulator with an attacker and a defender user interface.

The *Sparks II* reference discloses an attacker and a defender user interface **(Figure 3).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achieved

over great distances using a network, like the internet, where two people do not have to be in the same geographic location to play against each other in a simulation or a game ***(Sparks II, Col. 1 Lines 50-65)***.

6. Independent **Claim 9** is being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Sparks, II U.S. Patent 6,352,479.**

6.1 As regards independent **Claim 9** the *Gleichauf et al.* reference discloses a network configuration module **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a computer game.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test

the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

The *Sparks II* reference discloses a computer game **(Figures 1-12).**

It would have been obvious, to one of ordinary skill in the art, to have combined the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by playing a game using the game server disclosed in the *Sparks II* reference the player is able to be handicapped in a manner to determine the current level of skill and this is useful in determining if that particular individual is ready for operating at a particular skill level. In the manner described a computer security expert could determine if a particular person is qualified to receive a certification for a particular job protecting a computer network **(Sparks II, Figure 12)**.

7. Independent **Claim 10** and dependent **Claims 11, 13, 14 and 16** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Bergman et al. U.S. Patent 6,422,694** and in further view of **Smith, Jr. U.S. Patent 5,662,478.**

7.1 As regards independent **Claim 10** the *Gleichauf et al.* reference discloses a security modeling system **(Col. 2 Lines 47-50, Col. 4 Lines 20-43),** a network configuration module having network configuration data **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a mission objectives module coupled to the simulator used to determine network components that are involved in a specific attack scenario.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

The *Bergmann et al.* reference discloses determining network components that are involved in a specific attack scenario **(Figures 9-14, Col. 2 Lines 6-19).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Bergmann et al.* reference because *(motivation to combine)* the *Bergmann et al.* reference discloses that it is critical that the nodes where the attack originates be located or the attack will spread **(Bergmann et al. Col. 2 Lines 6-9).**

The *Smith Jr.* reference discloses mission objectives **(Col. 4 Lines 16-25).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Smith, Jr.* reference because *(motivation to combine)* the *Smith Jr.* reference discloses a method of reducing the time required

to lead a group through a creative *brain storming* process which results in more cost effective results **(Smith Jr. Col. 1 Lines 30-34).**

7.2 As regards dependent **Claim 11** the *Gleichauf et al.* reference discloses a database, including network vulnerability and exploitation data and attack data **(Figure 2 ITEM 80, Figure 3A ITEM 98, Figure 3B, 4 and 5, Col. 4 Lines 9-19, Col. 8 Lines 13-25).**

7.3 As regards dependent **Claim 13** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

7.4 As regards dependent **Claim 14** the *Gleichauf et al.* reference discloses goals, expectations and constraints **(Col. 1 Lines 1-67, Col. 2 Lines 1-65).**

7.5 As regards dependent **Claim 16** the *Gleichauf et al.* reference discloses a portable modeling system **(Figure 1 ITEMS 20, 22, 24 and 26).**

8. Dependent **Claims 12 and 15** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Bergman et al. U.S. Patent 6,422,694** and in further view of

Smith, Jr. U.S. Patent 5,662,478 and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

8.1 As regards independent **Claim 10** see the rejection in paragraph 7.1 above.

8.2 As regards dependent **Claim 12** the *Gleichauf et al.* reference does not expressly disclose database tables.

The *G2* reference discloses database tables **(Figure 3B and 3C).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

8.3 As regards dependent **Claim 15** the *Gleichauf et al.* reference does not expressly disclose receiving the network vulnerability, attack and exploitation data.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

9. Dependent **Claim 17** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in

further view of **Bergman et al. U.S. Patent 6,422,694** and in further view of **Smith, Jr. U.S. Patent 5,662,478** and in further view of **Sparks, II U.S. Patent 6,352,479.**

9.1 As regards independent **Claim 10** see paragraph 7.1 above.

9.2 As regards dependent **Claim 7** the *Gleichauf et al.* reference does not expressly disclose a simulator with an attacker and a defender user interface.

The *Sparks II* reference discloses an attacker and a defender user interface **(Figure 3).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achived over great distances using a network, like the internet, where two people do not have to be in the same geographic location to play against each other in a simulation or a game ***(Sparks II, Col. 1 Lines 50-65).***

10. Dependent **Claim 20** is rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **Ballard et al. U.S. Patent 4,937,825.**

10.1 As regards independent **Claim 18** see paragraph 3.1 above.

10.2 As regards dependent **Claim 20** the *Gleichauf et al.* reference does not expressly disclose network configuration files.

The *Ballard et al.* reference discloses network configuration files **(Col. 2 Lines 10-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ballard et al.* reference because *(motivation to combine)* the *Ballard et al.* reference discloses a method and apparatus for isolating and diagnosing problems in a data communications network **(Col. 1 Lines 58-68),** an artisan would be drawn to this teaching because it shows how to monitor and document the configuration of a data network which saves time and effort when trying to fix a problem.

11. Dependent **Claims 21, 22, 23 and 26** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

11.1 As regards independent **Claim 18,** see paragraph 3.1 above.

11.2 As regards dependent **Claim 21,** the *Gleichauf et al.* reference does not expressly disclose mission objectives.

The *Jackson* reference discloses mission objectives **(Page 7 "WINNING THE GAME").**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

11.3 As regards dependent **Claim 22,** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

11.4 As regards dependent **Claim 23**, the *Gleichauf et al.* reference does not expressly disclose dynamically interacting with an attacker.

The *Jackson* reference discloses interacting with an attacker **(Pages 2-7).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

11.5 As regards dependent **Claim 26** the *Gleichauf et al.* reference does not expressly disclose a score.

The *Jackson* reference discloses a score **(Page 7, WINNING THE GAME).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

12. Dependent **Claims 23, 24 and 25** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** herafter referred to as the *Jackson* reference and in further view of **Kurtzberg et al. U.S. Patent 5,961,644**.

12.1 As regards independent **Claim 18,** see paragraph 3.1 above.

12.2 As regards dependent **Claim 21,** see paragraph 11.2 above.

12.3 As regards dependent **Claim 22,** see paragraph 11.3 above.

12.4 As regards dependent **Claim 23,** the *Gleichauf et al.* reference does not expressly disclose dynamically interacting with an attacker.

The *Kurtzberg et al.* reference discloses dynamically interacting with an attacker **(Figure 6, Col. 3 Lines 20-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

12.5 As regards dependent **Claims 24 and 25** the *Gleichauf et al.* reference does not expressly disclose interacting in real time with a security modeling system.

The *Kurtzberg et al.* reference discloses interacting in real time with a security modeling system **(Figure 6, Col. 3 Lines 20-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

13. Dependent **Claim 27** is rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

13.1 As regards independent **Claim 18,** see paragraph 3.1 above.

13.2 As regards dependent **Claim 21,** see paragraph 11.2 above.

13.3 As regards dependent **Claim 27** the *Gleichauf et al.* reference does not expressly disclose updating the vulnerabilities data base.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

14. Independent **Claim 28** and dependent **Claims 29 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **"Simulated Attack for Real Network Security" by Johna Till Johnson**, *hereafter referred to as the Johnson* reference, and in further view of **Kurtzberg et al. U.S. Patent 5,961,644** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

14.1 As regards independent **Claim 28** the *Gleichauf et al.* reference discloses a method of opposing network attackers **(Figure 1, ITEMS 40, 42, 44 and 46, Figure 2 ITEM 80, Col. 1 Lines 10-21),** receiving a network configuration comprising hardware and software component information **(Figure 2,** *note device type [hardware] and services [software],* **Col. 4 Lines 20-42, Col. 5 Lines 14-26),** determining results as a function of network configuration, and stored vulnerability data for the described computer hardware and software components **(Figure 1 Item 26, Figures 3A-5, Col. 8 Lines 12-25).**

However, the *Gleichauf et al.* reference does not expressly disclose; simulated network attacks, mission objectives, receiving commands from a network attacker and responding to the attack.

The *Johnson* reference discloses a simulated network attack **(Pages 31-32).**

It would have been obvious, to one of ordinary skill in the at, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Johnson* reference because, *(motivation to combine)* the *Johnson* reference discloses a good method for preventing unauthorized access to a data network **(Johnson page 31-32).**

The *Kurtzberg et al.* reference discloses receiving commands from a network attacker **(Figure 6, Col. 3Lines 20-28),** and responding to the attack **(Col. 3 Lines 40-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

The *Jackson* reference discloses mission objectives **(Page 7 WINNING THE GAME).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

14.2 As regards dependent **Claim 29** the *Gleichauf et al.* reference does not expressly disclose defender commands.

The *Kurtzberg et al.* reference discloses defender commands **(Figure 6, *YES result*).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

14.3 As regards dependent **Claim 30** the *Gleichauf et al.* reference does not expressly disclose receiving critical resource information.

The *Johnson* reference discloses critical resource information **(Page 31, specified set of IP addresses).**

It would have been obvious, to one of ordinary skill in the at, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Johnson* reference because, *(motivation to combine)* the *Johnson* reference discloses a good method for preventing unauthorized access to a data network **(Johnson page 31-32).**

15. Dependent **Claims 31-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **"Simulated Attack for Real Network Security" by Johna Till Johnson**, *hereafter referred to as the Johnson* reference, and in further view of **Kurtzberg et al. U.S. Patent 5,961,644** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference and in further view of **Porras et al. U.S. Patent 6,321,338.**

15.1 As regards independent **Claim 28** see paragraph 14.1 above.

15.2 As regards dependent **Claim 31** the *Gleichauf et al.* reference does not expressly disclose a graphical user interface.

The *Porras et al.* reference discloses a GUI **(Figure 5 Items 54, 50 and 58, Col. 14 Lines 50-58).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Porras et al.* reference

because *(motivation to combine)* the ability to do statistical analysis on packet usage allows for detection of subtle network intrusions not easily detectable using non-statistical means **(Porras et al. Col. 1 Lines 42-54).**

15.3 As regards dependent **Claim 32** the *Gleichauf et al.* reference does not expressly discloses a security score.

The *Porras et al.* reference discloses a security score **(Col. 11 Lines 57-67, Col. 12 Lines 1-6).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Porras et al.* reference because *(motivation to combine)* the ability to do statistical analysis on packet usage allows for detection of subtle network intrusions not easily detectable using non-statistical means **(Porras et al. Col. 1 Lines 42-54).**

15.4 As regards dependent **Claim 33** the *Gleichauf et al.* reference does not expressly disclose receiving attack commands that change services or nodes and that exploit vulnerabilities.

The *Kurtzberg et al.* reference discloses receiving attack commands that change services or nodes and that exploit vulnerabilities **(Figure 6, Col. 3 Lines 40-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

16. Independent **Claims 34 and 40** and dependent **Claims 35-38, 41 and 42** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **"Simulated Attack for Real Network Security" by Johna Till Johnson**, *hereafter referred to as the Johnson* reference in view of **Porras et al. U.S. Patent 6,321,338** and in further view of **Gleichauf et al. U.S. Patent 6,282,546.**

16.1 As regards independent **Claims 34 and 40** the *Johnson* reference discloses a security modeling system for simulating networks and to determine network components that are involved in a specific attack scenario including configuration data **(Pages 31-32).**

However, the *Johnson* reference does not expressly disclose, a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables as well as a graphical user interface.

The *Gleichauf et al.* reference discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables **(Figure 1, Figures 3A, 3B, 3C, 3D,)** and configuration tables **(TABLE 1 Col. 5 Lines 45-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because, *(motivation to combine)* organizing data into tables is well known in the art and the *Gleichauf et al.* reference discloses good methods of organizing data related to Network Security Vulnerability testing in such a manner that allows for flexibility and efficiency **(*Gleichauf et al.* Col. 1 Lines 58-63).**

The *Porras et al.* reference discloses the use of a Graphical User Interface **(Col. 14 Lines 51-58).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Porras et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

16.2 As regards dependent **Claims 35 and 41** the *Johnson* reference does not expressly disclose mission tables or files.

The *Gleichauf et al.* reference discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables **(Figure 1, Figures 3A, 3B, 3C, 3D,)** and configuration tables **(TABLE 1 Col. 5 Lines 45-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because, *(motivation to combine)* organizing data into tables is well known in the art and the *Gleichauf et al.* reference discloses good methods of organizing data related to Network Security Vulnerability testing in such a manner that allows for flexibility and efficiency **(*Gleichauf et al.* Col. 1 Lines 58-63).**

16.3 As regards dependent **Claim 36** the *Johnson* reference does not expressly disclose service tables.

The *Gleichauf et al.* reference discloses a service table **(Figure 5B).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* the ability to catalog services in a database is useful because there can be a record of which services are authorized and the data base can be used as an audit tool to determine what has happened after an attack ***(Gleichauf et al. Col. 2 Lines 36-40).***

16.4 As regards dependent **Claim 37** the *Johnson* reference does not expressly disclose configuration tables, defense tables, node tables, routing tables and password tables.

The *Gleichauf et al.* reference discloses configuration tables, defense tables, node tables, routing tables and password tables **(Col. 5 Lines 8-36).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* the ability to catalog services in a database is useful because there can be a record of which services are authorized and the data base can be used as an audit tool to determine what has happened after an attack ***(Gleichauf et al. Col. 2 Lines 36-40).***

16.5 As regards dependent **Claim 38** the *Johnson* reference does not expressly disclose transmitting real-time network information

The *Porras et al.* reference discloses real-time monitoring **(Col. 3 Lines 42-54).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Porras et al.* reference because, *(motivation to combine)* to be able to monitor events in real-time the amount of damage from a network intrusion can be minimized.

16.6 As regards dependent **Claim 42** the *Johnson* reference does not expressly disclose determining which network components are involved in a specific network attack.

The *Gleichauf et al.* reference discloses determining which network components are involved in a specific network attack **(Figures 6A, 6B, Col. 7 Lines 29-42).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* different devices on a computer network have different vulnerabilities and it is useful to have a central database to distinguish which device is being attacked and what vulnerabilities are present on that specific platform ***(Gleichauf et al. Col. 7 Lines 29-42).***

17. Independent **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

17.1 As regards independent **Claim 9** the *Gleichauf et al.* reference discloses a network configuration module **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a computer game.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

The *Jackson* reference discloses a game **(Pages 1-8).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

Conclusion

18. Claims 1-42 have been presented for reconsideration. Claims 1-42 have been reconsidered and rejected.

18.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. **Fox Et al. U.S. Patent 6,535,227** discloses a system for assessing the security posture of a network.

2. **Kingsford et al. U.S. Patent 6,574,737** discloses a system for penetrating a computer network.

18.2 An updated search has revealed new art, as a result of the new art rejections this action is made **NON-FINAL.**

18.3 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dwin M Craig whose telephone number is 703 305-7150. The examiner can normally be reached on 9:00 - 5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kevin Teska can be reached on 703 305-9704. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 305-3900.

DMC
August 4, 2003